



## **Note d'analyse**

### **Le fichage**

Un outil sans limites au service du contrôle des frontières ?

Septembre 2019

## Table des matières

<b>CONTEXTE – L'ÉVOLUTION DES FICHIERS A L'AUNE DU RENFORCEMENT DES POLITIQUES MIGRATOIRES .....</b>	<b>4</b>
<b>DES FICHIERS AU SERVICE DES POLITIQUES MIGRATOIRES .....</b>	<b>6</b>
La multiplication de fichiers de contrôle des personnes étrangères : un maillage complexe en constant développement.....	6
1) Qu'est-ce qu'un fichier ? .....	6
2) Un maillage complexe en pleine extension .....	8
Les fichiers comme outil d'identification et de contrôle migratoire .....	11
1) Identifier pour mieux catégoriser et « trier » .....	11
2) Les fichiers comme vecteurs d'une image négative de « l'étranger ».....	13
<b>LES FICHIERS COMME OUTIL DE CONTRÔLE DES FRONTIÈRES .....</b>	<b>14</b>
Le recours aux fichiers dès la procédure de visa.....	14
1) La naissance des visas .....	14
2) Les fichiers consultés en amont de l'arrivée en France .....	15
L'utilisation des fichiers aux frontières extérieures françaises.....	17
1) L'usage des fichiers par les services administratifs et de police... ..	17
... A l'arrivée aux frontières et pendant le maintien en zone d'attente.....	17
... A la fin du maintien en zone d'attente .....	18
Le cas particulier des demandes d'asile .....	19
2) La prise en compte des fichiers par les juridictions .....	20
Entre les mailles des fichiers : les failles .....	21
La banalisation du fichage lors des contrôles aux frontières intérieures .....	23
<b>LE FRANCHISSEMENT DES FRONTIÈRES PAR LES CITOYENS EUROPÉENS : LES DERIVES DU FICHAGE</b>	<b>25</b>

## **Abréviations**

ANAFE	Association nationale d'assistance aux frontières pour les étrangers
CC	Conseil constitutionnel
CE	Commission européenne
CEDH	Cour européenne des droits de l'homme
CESEDA	Code de l'entrée et du séjour des étrangers et du droit d'asile
CGLPL	Contrôleur général des lieux de privation de liberté
CNIL	Commission nationale de l'informatique et des libertés
CRA	Centre de rétention administrative
JLD	Juge des libertés et de la détention
OFII	Office français de l'immigration et de l'intégration
OFPPA	Office français de protection des réfugiés et apatrides
ONU	Organisation des Nations-unies
PAF	Police aux frontières
RGPD	Règlement général de protection des données personnelles
TA	Tribunal administratif
TGI	Tribunal de grande instance
UE	Union européenne
ZA	Zone d'attente
ZAPI	Zone d'attente pour personnes en instance (Roissy)

### **Fichiers**

AGDREF 2	Application de gestion des dossiers des ressortissants étrangers en France
API-PNR	Advance passenger information - personal name record
DNA	Dispositif national d'accueil des demandes d'asile
EURODAC	EU Biometric data base
EUROPOL	European police office
FAED	Fichier automatisé des empreintes digitales
Fichier S	Atteinte à la sûreté de l'Etat
FNAEG	Fichier national automatisé des empreintes génétiques
FPR	Fichier des personnes recherchées
GESTEL	Gestion de l'éloignement
GIPI	Gestion informatisée des procédures d'immigration
INEREC	Instruction et recours
INTERPOL	Organisation internationale de police criminelle
OSCAR	Outil de statistique et de contrôle de l'aide au retour
RMV2	Réseau mondial visa
SILCF	Système informatisé concourant au dispositif de lutte contre les fraudes
SIS II	Système d'information Schengen
TAJ	Traitement d'antécédents judiciaires
TES	Titre électronique sécurisé
VIS	Visa information system
VISABIO	Visa biométrique

### **Langage épïcène**

L'Anafé a choisi d'utiliser un langage « non sexiste » par soucis d'égalité entre les genres. Cette note est donc rédigée dans la mesure du possible en utilisant le langage épïcène. Par exemple, le choix a été fait d'écrire « personnes en migration » ou « personnes exilées » plutôt que « migrants ». Cependant pour des commodités de lecture, le « point médian » n'est pas utilisé.

## **CONTEXTE – L'ÉVOLUTION DES FICHIERS A L'AUNE DU RENFORCEMENT DES POLITIQUES MIGRATOIRES**

Si le droit international proclame le droit de chaque personne de quitter tout pays, y compris le sien, et d'y revenir, il protège également toute personne en migration contre les mauvais traitements et violations de ses droits fondamentaux.

Or, la libre circulation à l'intérieur de l'espace Schengen s'accompagne d'une surveillance accrue de ses frontières extérieures et de l'externalisation de celles-ci, avec l'édification de murs, le contrôle militarisé des frontières, la mise en place de hotspots, les refus de délivrer des visas, le maintien des visas de transit aéroportuaire, la multiplication des fichiers, les retours forcés, l'enfermement... Les personnes en migration et en situation d'exil sont présentées comme une menace dont il faut se défendre en développant de façon drastique, depuis la fin des années 90, la machine législative et politique en Europe.

En définitive, la « crise migratoire » mise sur le devant de la scène politique européenne depuis 2015 est précisément une crise des politiques migratoires européennes.

En stigmatisant les personnes migrantes comme des indésirables, le racisme et la xénophobie sont alimentés, et l'Europe déploie un véritable arsenal contre un ennemi qu'elle s'est inventé, mais aussi et de plus en plus vis-à-vis des acteurs de la solidarité.

La traversée des frontières par des personnes étrangères est un « outil » politique et médiatique, utilisé pour faire accepter à la population toutes les mesures toujours plus attentatoires aux libertés individuelles, au nom par exemple de la lutte contre le terrorisme. Le prétexte sécuritaire est érigé en étendard et il est systématiquement brandi dans les discours politiques, assimilant ainsi migration et criminalité, non seulement pour des effets d'annonce mais de plus en plus dans les législations.

Les personnes étrangères font depuis longtemps l'objet de mesures de contrôle et de surveillance. Pourtant, un changement de perspective s'est opéré pour s'adapter aux grands changements des politiques européennes vers une criminalisation croissante de ces personnes, en lien avec le développement constant des nouvelles technologies. L'utilisation exponentielle des fichiers est destinée à identifier, catégoriser, contrôler, éloigner et exclure. Et si le fichage est utilisé pour bloquer les personnes sur leurs parcours migratoires, il est aussi de plus en plus utilisé pour entraver les déplacements à l'intérieur de l'Union et l'action de militants européens qui entendent apporter leur soutien aux personnes exilées.

Quelles sont les limites à ce développement ? Les possibilités techniques et numériques semblent illimitées et favorisent alors un véritable « business » du fichage.

Concrètement, il existe pléthore de fichiers. Leur complexité tient au fait qu'ils sont nombreux, mais également à leur superposition. De ce maillage opaque naît une certaine insécurité juridique pour les personnes visées.

Parallèlement à la multiplication des fichiers de tout type et de toute nature, ce sont désormais des questions liées à leur interconnexion<sup>1</sup>, à leurs failles qui sont soulevées et aux abus dans leur utilisation, notamment aux risques d'atteintes aux droits fondamentaux et aux libertés publiques.

---

<sup>1</sup> L'interconnexion est le partage de données contenues dans plusieurs fichiers, c'est-à-dire « l'objet même d'un traitement qui permet d'accéder à, d'exploiter, et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu. ([Définition du Conseil d'Etat, arrêt n°317182 du 19 juillet 2010](#)).

Le 5 février 2019, un accord provisoire a été signé entre la présidence du Conseil européen et le Parlement européen sur l'interopérabilité<sup>2</sup> des systèmes d'information au niveau du continent pour renforcer les contrôles aux frontières de l'Union.

Il doit permettre l'unification de six registres avec des données d'identification alphanumériques et biométriques (empreintes digitales et images faciales) de personnes non membres de l'UE. Pourront ainsi accéder à la nouvelle base de données les forces de police des États membres, mais aussi les responsables d'Interpol, d'Europol et, dans de nombreux cas, même les gardes-frontières de l'agence européenne Frontex<sup>3</sup>. Ils pourront rechercher des personnes par nom, par empreinte digitale ou faciale, et croiser les informations de plusieurs bases de données. Cela revient donc à mettre sur le même plan autorités de contrôle aux frontières et autorités répressives. De la même façon, cela revient à mettre à tort sur le même plan lutte contre la criminalité et lutte contre l'immigration dite irrégulière.

En 2020, le système Entry Exit (l'une des trois nouvelles bases de données centralisées avec interopérabilité) entrera en vigueur. Il oblige chaque État membre à collecter les empreintes digitales et les images de visages des Européens entrant et sortant de l'Union, et d'alerter lorsque les permis de résidence expirent. Ce sera ensuite au tour d'Etias (Système européen d'information de voyage et d'autorisation), le nouveau registre qui établit un examen préventif des demandes d'entrée, même pour les personnes venant de pays qui n'ont pas besoin de visa pour entrer dans l'UE.

La justification est toujours de « *protéger les citoyens européens du terrorisme international* », mais il n'existe pas véritablement de donnée ou étude sur la manière dont les nouveaux registres de données biométriques et leur interconnexion peuvent contribuer à cet objectif.

En conséquence, chaque frontière, aéroportuaire, portuaire ou terrestre, devrait être équipée à terme de lecteurs d'empreintes digitales et d'images faciales. Et franchissant encore une étape supplémentaire, favorisée par le développement des nouvelles technologies, des détecteurs de mensonge sont expérimentés aux frontières extérieures de l'Europe. Le « système iBorder » ayant ainsi pour objectif d'accélérer les contrôles et de renforcer la sécurité<sup>4</sup>.

A tous les niveaux, le fichage intensif est devenu un outil de contrôle des frontières. Il s'agit ici d'examiner les objectifs, le fonctionnement et les conséquences d'un maillage de 21 fichiers nationaux, européens et internationaux utilisés dans le cadre du contrôle des frontières<sup>5</sup>, à l'égard des personnes étrangères mais également de citoyens européens. Cette note n'a pas vocation à être exhaustive mais vise à donner des clés de compréhension et d'analyse.

---

<sup>2</sup> L'interopérabilité est la capacité des systèmes d'information à échanger des données et à permettre le partage d'informations ([Définition de la Commission européenne](#), COM/2016/0205 final).

<sup>3</sup> L'agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne, surnommée Frontex est une agence de l'Union européenne ayant existé entre 2004 et 2016, date à laquelle elle a été remplacée par l'Agence européenne de garde-frontières et de garde-côtes. Pour en savoir plus, voir le site de la campagne [Frontexit](#) dont l'objectif est d'informer et de dénoncer les dérives des opérations de Frontex en termes de droits humains.

<sup>4</sup> « [Des détecteurs de mensonge expérimentés aux frontières extérieures de l'Europe](#) », Le Monde, 31 août 2019.

<sup>5</sup> Anafé, [La boîte à fichiers](#), avril 2019.

## DES FICHIERS AU SERVICE DES POLITIQUES MIGRATOIRES

### La multiplication de fichiers de contrôle des personnes étrangères : un maillage complexe en constant développement

#### 1) Qu'est-ce qu'un fichier ?

Un fichier est un « *ensemble structurel de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* »<sup>6</sup>.

En d'autres termes, un fichier est une base de données dans laquelle sont enregistrées et traitées des données personnelles (collecte, conservation, exploitation, modification, communication, archivage, destruction) selon un ou des objectifs déterminés. Il existe un grand nombre de fichiers, avec une superposition de fichiers nationaux, européens et internationaux, qui parfois s'alimentent entre eux<sup>7</sup>.

Depuis les années 1980, on assiste à un large essor de fichiers nationaux<sup>8</sup>. Dans le même temps, les fichiers européens se développent<sup>9</sup>. De nouveaux types de données ont également été collectés et enregistrés dans les fichiers, tels que les données biométriques, au sein de fichiers européens (EURODAC, SIS II) ou nationaux (FAED, FNAEG)<sup>10</sup>.

Le développement intensif des fichiers a contraint les instances nationales et internationales à encadrer leur création et utilisation. En France, le premier texte visant à réglementer le fichage et à poser les bases d'une protection des libertés individuelles est la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi a créé une autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL), et institue pour la première fois un contrôle a priori d'une autorité extérieure à la police sur les bases de données que gère cette dernière. Cette loi a dû être modifiée à plusieurs reprises pour transposer des directives européennes<sup>11</sup> ou l'adapter à un règlement européen<sup>12</sup>. La réglementation européenne en matière de fichage a longtemps reposé sur la directive 95/46/CE du 24 octobre 1995<sup>13</sup> et la décision-cadre du 27 novembre 2008<sup>14</sup>. Ces

---

<sup>6</sup> Article 4, 6) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

<sup>7</sup> Par exemple, le fichier SIS II est alimenté par les signalements du FPR.

<sup>8</sup> Entre autres, le fichier des personnes recherchées (FPR), le fichier automatisé des empreintes digitales (FAED), le fichier national automatisé des empreintes génétiques (FNAEG).

<sup>9</sup> Notamment le Système d'information Schengen I et II (SIS) et Eurodac.

<sup>10</sup> Pierre Piazza, « [L'extension des fichiers de sécurité publique](#) », *Hermès, La Revue*, 2009/1 (n° 53), p. 67-74.

<sup>11</sup> La loi n°2004-801 du 6 août 2004 a transposé la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et l'ordonnance n°2011-1012 du 24 août 2011 a transposé la directive 2009/136/CE du 25 novembre 2009.

<sup>12</sup> La loi n°2018-493 du 20 juin 2018 a modifié la loi du 6 janvier 1978 pour l'adapter au RGPD.

<sup>13</sup> Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

<sup>14</sup> Décision-cadre 2008/909/JAI du Conseil du 27 novembre 2008 concernant l'application du principe de reconnaissance mutuelle aux jugements en matière pénale prononçant des peines ou des mesures privatives de liberté aux fins de leur exécution dans l'Union européenne.

deux textes ont été abrogés et remplacés par deux nouveaux. Le premier est le règlement européen du 27 avril 2016, dit « Règlement général de protection des données personnelles »<sup>15</sup>, entré en vigueur le 25 mai 2018. Le second texte est la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des données personnelles à des fins répressives, dite « Directive police »<sup>16</sup>, s'appliquant aux bases de données relevant de la coopération policière et judiciaire pénale. La Charte des droits fondamentaux de l'Union européenne<sup>17</sup> contient également dans son article 8 des dispositions spécifiques à la protection des données à caractère personnel.

Les fichiers répondent à des objectifs définis par la norme qui les instaure. Ainsi, les données qui y sont enregistrées et les personnes ou entités y ayant accès sont limitativement énumérés. S'il existe des interconnexions avec d'autres fichiers, cela doit également être prévu. Ces données ne peuvent être conservées dans le fichier que pendant une durée limitée. Le texte doit également préciser les droits des personnes fichées, c'est-à-dire si elles disposent ou non d'un droit d'opposition au traitement de leurs données personnelles, d'un droit d'information et d'accès direct ou indirect, de rectification, de verrouillage ou de suppression des données.

Pour comprendre le fonctionnement d'un fichier, l'exemple du fichier européen SIS II est éclairant. Considéré comme le « *premier grand fichier de police européen, moteur des autres fichiers de sécurité* »<sup>18</sup>, le fichier SIS II remplace le SIS I depuis le Règlement (CE) n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II). Initialement mis en place pour « compenser » la libre circulation des personnes dans l'espace Schengen, le SIS II a pour objectif « *d'assurer un niveau élevé de sécurité* », « *la préservation de la sécurité et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres*<sup>19</sup> » de l'Union européenne. Il permet aux autorités nationales, notamment les forces de police et les gardes-frontières, de saisir et de consulter des signalements concernant des personnes ou des objets. Il est alimenté par plusieurs fichiers, dont notamment le fichier des personnes recherchées (FPR). Le FPR est un fichier national recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique. Il permet de faciliter les recherches de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives.

---

<sup>15</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

<sup>16</sup> Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

<sup>17</sup> Charte des droits fondamentaux de l'Union européenne, article 8 « Protection des données à caractère personnel » :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

<sup>18</sup> Sylvia Preuss-Laussinotte, « [L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité](#) », in *Cultures & Conflits* [En ligne], 74 | été 2009, mis en ligne le 28 octobre 2010.

<sup>19</sup> Article premier du règlement (CE) n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du SIS II.

L'architecture complexe du SIS II s'articule en un système central contenant la base de données du SIS II (le C-SIS II central), des systèmes nationaux dans chaque État membre (le N-SIS II), et une infrastructure de communication entre le système central et les systèmes nationaux.

Il contient des informations sur des personnes recherchées ou disparues, des personnes sous surveillance policière et des personnes non ressortissantes d'un État membre de l'espace Schengen auxquelles l'entrée sur le territoire Schengen est interdite, ainsi que des informations sur des véhicules et objets volés ou disparus, comme des documents d'identité, des certificats d'immatriculation de véhicules et des plaques d'immatriculation de véhicules. Les données enregistrées sont nominatives mais également biométriques (empreintes digitales notamment).

Au niveau français, les agents du bureau SIRENE gérant la partie nationale du fichier, les services de l'administration centrale du ministère de l'intérieur compétents en matière d'entrée, de séjour et d'éloignement ou encore les agents consulaires font partie des acteurs ayant accès à ce fichier. A l'échelle européenne, d'autres types d'acteurs, dont Europol, peuvent également y accéder.

Les personnes étrangères peuvent être dans deux sortes de fichiers : les fichiers uniquement consacrés aux personnes étrangères, relatifs à l'entrée, au séjour, à la procédure d'asile ou encore à l'éloignement du territoire français d'une part, et les fichiers pouvant contenir également des données de ressortissants français comme les fichiers de police (FAED, FNAEG, FPR, TAJ...) d'autre part.

Cette multiplication et variation des fichiers est en concordance avec l'évolution du contrôle des frontières et des conditions d'entrée sur le territoire Schengen lié à un contexte politique de plus en plus répressif. Les États européens externalisent leurs frontières en déplaçant le contrôle directement dans les pays de départ et à toutes les étapes des parcours migratoires avant le contrôle aux frontières à proprement parler pour les personnes qui parviendraient à arriver aux portes de l'Europe (peu importe le motif).

## **2) Un maillage complexe en pleine extension**

Le maillage que constitue l'ensemble des fichiers s'est complexifié par la création croissante de fichiers, mais également par l'évolution même des fichiers existants.

Les fichiers vont vers une augmentation des données qu'ils peuvent enregistrer par rapport au moment de leur mise en œuvre initiale. C'est le cas pour le fichier SIS lors du passage du SIS I au SIS II, de nouvelles données pouvant être collectées ont été prévues par le Règlement 1987/2006, telles que les empreintes digitales, la photographie de la personne ou encore la référence à la décision qui est à l'origine du signalement.

Dans le même sens, on peut observer un élargissement des champs des fichiers. A titre d'exemple, le FNAEG (Fichier national automatisé des empreintes génétiques), initialement envisagé en 1998 dans le but d'identifier les auteurs d'infractions sexuelles, a progressivement été élargi à l'identification des auteurs d'atteintes aux personnes et aux biens les plus graves en 2001, puis à presque l'ensemble des infractions en 2003.

Plus récemment, la Commission européenne dans le cadre d'un projet de refonte du système « Dublin » a proposé une refonte du règlement Eurodac et d'élargir l'objet du fichier Eurodac. Ce fichier contient actuellement des données relatives aux demandes d'asile et aux personnes appréhendées lors du franchissement d'une frontière extérieure de l'Union européenne, dans le but de faciliter la mise en œuvre du règlement « Dublin » sur la



détermination de l'État responsable de l'examen d'une demande d'asile. Dans une communication du 4 mai 2016, la Commission européenne propose une nouvelle extension du champ d'application du règlement « Eurodac », afin de permettre aux États membres de stocker et de rechercher des données relatives aux personnes ressortissantes de pays tiers ou apatrides, ne relevant pas de la protection internationale et en situation irrégulière dans l'Union, de sorte qu'elles puissent être identifiées à des fins de retour ou de réadmission<sup>20</sup>. Portée en même temps que le projet de révision du règlement « Dublin », cette proposition devrait également permettre aux États membres, « *dans le plein respect des règles en matière de protection des données* », de stocker davantage de données à caractère personnel, telles que le nom, la date de naissance, la nationalité, des éléments d'identification ou des documents de voyage, et l'image faciale.

Le développement d'Eurodac dépasse dès lors très largement son champ d'application initial.

Les fichiers peuvent être interconnectés entre eux en procédant à un partage de données. La Commission européenne emploie le terme d'« *interopérabilité* » entre plusieurs fichiers<sup>21</sup>. De nombreuses interconnexions existent déjà entre fichiers d'échelles différentes. Par exemple, le fichier européen VIS (Système d'information sur les visas) utilisé pour l'examen de demande de visas de court séjour est interconnecté avec les fichiers nationaux VISABIO (Visa biométrique) et RMV 2 (Réseau mondial visa), ce qui permet un échange d'informations entre le ministère de l'intérieur et les autorités des différents États de l'espace Schengen.

Mais la tendance est à une interconnexion encore plus poussée entre les fichiers, dont des fichiers déjà existants. Le dernier projet en ce sens a été initié par l'Union européenne. Par le biais de deux règlements européens récents<sup>22</sup>, établissant un cadre pour l'interopérabilité des systèmes d'information de l'UE respectivement dans le domaine des frontières et des visas, et dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration, les États membres prévoient également une interconnexion entre des fichiers européens.

Les fichiers Eurodac, SIS II et VIS sont amenés à « *se compléter mutuellement* ». Pour cela, doivent être créés un portail de recherche européen, un service partagé d'établissement de correspondances biométriques, un répertoire commun de données d'identité, ainsi qu'un détecteur d'identités multiples. Les objectifs affichés par cette interopérabilité sont, entre autres, d'« *améliorer l'efficacité et l'efficience des vérifications aux frontières extérieures* » et « *de contribuer à la prévention de l'immigration illégale et à la lutte contre celle-ci* ».

---

<sup>20</sup> Proposition de règlement du Parlement européen et du Conseil relatif à la création d'« Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) n°604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride, et de l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives (refonte).

<sup>21</sup> Communication au Parlement européen et au Conseil, *Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité*, COM/2016/0205 final.

<sup>22</sup> - Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil.

- Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816.

L'élargissement de l'accès au contenu de fichiers facilite les croisements d'un fichier à un autre, mais également d'un pays à un autre. Au sein de l'Union européenne, le traité de Prüm vise à « *intensifier la coopération transfrontalière [...] en particulier l'échange d'informations* » entre les États parties<sup>23</sup>. Il est par ailleurs prévu dans la décision n°2008/615/JAI du Conseil du 23 juin 2008<sup>24</sup> la création de bases de données nationales comprenant des profils ADN et l'accès automatisé à ces différentes bases de données par les différents États membres de l'Union européenne. Les États membres ont accès aux données contenues dans les fichiers nationaux d'identification par empreintes digitales d'autres États membres. Ainsi, les États européens peuvent avoir accès aux données des personnes inscrites dans le fichier français FNAEG.

Cet élargissement d'accès aux données ne se limite pas aux États, mais également à des organisations internationales et des États tiers.

A titre d'exemple, Europol qui est une organisation intergouvernementale, composée des services de police et des douanes des États membres, chargée de faciliter la coopération policière européenne. Son rôle est de faciliter l'échange d'informations entre les autorités nationales, en mettant en œuvre un système de recueil d'informations. Europol a accès à plusieurs bases de données européennes.

Depuis le 20 juillet 2015, Europol peut demander la comparaison de données dactyloscopiques (empreintes digitales) contenues dans Eurodac à des fins répressives, dans le cadre d'une procédure pénale particulière<sup>25</sup>. Europol a également accès au SIS II et peut consulter le VIS dans les limites de ses missions<sup>26</sup>.

Europol ayant conclu des accords d'échange de données avec des pays tiers, ceux-ci peuvent de fait avoir accès aux données contenues dans les fichiers européens (l'information sur les fichiers concernés et selon quelles modalités n'est pas facile à trouver). La communication de données personnelles à des pays tiers est déjà explicitement prévu par le Règlement (CE) n°767/2008 pour le fichier VIS sous certaines conditions<sup>27</sup>.

La complexité de ce maillage fait d'interconnexions tient également au fait qu'il est très difficile d'identifier chaque fichier séparément. L'élargissement de l'accès aux fichiers par

---

<sup>23</sup> Traité de Prüm du 27 mai 2005 entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière.

<sup>24</sup> Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JOUE L 218/129, 13 août 2008.

<sup>25</sup> Règlement (UE) n°603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à la création d'Eurodac pour la comparaison des empreintes digitales aux fins de l'application efficace du règlement (UE) no 604/2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et Europol à des fins répressives, et modifiant le règlement (UE) no 1077/2011 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (refonte).

<sup>26</sup> Décision 2008/633/JAI du Conseil du 23 juin 2008 concernant l'accès en consultation du système d'information sur les visas (VIS) par les autorités désignées des États membres et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, JOUE L 218/129, 13 août 2008.

<sup>27</sup> Article 31 du Règlement (CE) n°767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).

différents acteurs complique l'identification du responsable du fichier, des personnes et entités pouvant l'alimenter ou seulement le consulter. Cela est encore plus ardu du fait que les informations concernant chaque fichier<sup>28</sup> sont difficiles à trouver, de manière claire, précise et complète.

De plus, pour certains fichiers, le droit à l'information de la personne sur l'inscription de ses données personnelles dans un fichier n'est pas prévu, entravant alors le droit d'accès au fichier et sa contestation éventuelle.

C'est notamment le cas pour les personnes faisant l'objet d'une « fiche S », qui est un des 21 sous-fichiers du FPR. Pour d'autres, le droit d'accès et de communication de ses données est soumis à une longue procédure, passant par plusieurs étapes et interlocuteurs, avec parfois des recours prévus en cas de rejet de leur demande. A titre d'exemple, pour pouvoir accéder à ses données enregistrées dans le TAJ (Traitement d'antécédents judiciaires), la personne doit faire une demande auprès du ministère de l'intérieur. S'il répond défavorablement ou ne répond pas dans un délai de deux mois, la personne doit communiquer à la CNIL une copie de son titre d'identité ou extrait d'acte de naissance et la copie du courrier défavorable du ministère de l'intérieur ou du courrier de demande initiale en cas d'absence de réponse. Les délais de réponse de la CNIL sont cependant très longs (plus de 18 mois).

L'accès aux informations concernant ses données enregistrées dans un fichier peut donc être un véritable parcours kafkaïen.

## Les fichiers comme outil d'identification et de contrôle migratoire

### 1) Identifier pour mieux catégoriser et « trier »

La facilitation d'échanges de données par la multiplication des interconnexions entre les fichiers et par l'élargissement de l'accès à ceux-ci participe à l'objectif implicite de contrôle des migrations.

Lorsqu'un fichier est créé, ses objectifs doivent être explicitement définis. Cependant, au-delà de ces objectifs affichés, se cachent en réalité d'autres objectifs. Les fichiers sont utilisés à toutes les échelles (nationale, européenne, internationale) comme un outil de gestion pour l'application des politiques migratoires européennes et nationales.

Un changement d'échelle et de perspective s'est opéré pour s'adapter aux grands changements politiques. Les grandes politiques européennes en matière de migration ont été accompagnées de création de fichiers. Ce fût le cas pour le fichier SIS II, créé par la convention du 19 juin 1990 portant application de l'accord de Schengen du 14 juin 1985.

De même, afin de pouvoir appliquer le système européen de détermination de l'État responsable de l'examen d'une demande d'asile institué par la convention dite «de Dublin » du 15 juin 1990, la base de données Eurodac a été mise en œuvre. Enfin, la mise en place d'une politique européenne commune de visas avec le visa uniforme Schengen a abouti à la création du fichier VIS pour pouvoir gérer et appliquer cette politique.

---

<sup>28</sup> Des informations comme la date de création, les objectifs, le contenu des données, les critères d'inscription dans le fichier, les autorités compétentes, l'accès au fichier, la durée de conservation, l'interconnexion avec d'autres fichiers, les lois qui régissent le fichier, ou encore comment obtenir la communication et la rectification des données.

Des fichiers existent pour toutes les étapes des parcours migratoires, que ce soit de la demande de visa jusqu'à l'éloignement du territoire, en passant par le contrôle à la frontière, les démarches de séjour ou de demande d'asile.

Le parcours d'une personne étrangère est « jalonné de fichiers »<sup>29</sup>. Ainsi, « il devient possible de repérer, de localiser et de suivre les personnes à distance par le biais d'un strict contrôle de leurs mouvements dans l'espace et le temps »<sup>30</sup>. Les fichiers sont utilisés pour contrôler les frontières et deviennent un rempart à leur franchissement. On assiste à une dématérialisation de la frontière, puisqu'il devient possible « d'identifier une personne en tout lieu et à tout moment, c'est-à-dire l'élargissement de la notion de surveillance au-delà des frontières institutionnelles et territoriales »<sup>31</sup>.

Ce contrôle intégral des déplacements des personnes est rattaché à l'idée que la migration représente un risque. Les personnes étrangères sont identifiées et catégorisées comme telles par leur fichage et il devient ainsi plus simple de surveiller leurs déplacements. Comme le relève Ségolène Barbou Des Places, « certains étrangers, pour de multiples raisons, cherchent à cacher leur identité. Le besoin d'identification devient donc un enjeu dans la politique des étrangers »<sup>32</sup>.

La biométrie permet d'identifier les personnes en fonction de leurs caractéristiques biologiques telles que les empreintes digitales ou les traits de leur visage. Le recours à la biométrie<sup>33</sup> au niveau européen, ayant débuté avec le fichier Eurodac et s'étant généralisé avec les fichiers SIS et VIS, participe de cette volonté d'utiliser les fichiers comme « outil d'identification des étrangers »<sup>34</sup>. Considérée plus fiable que l'identification visuelle par des données photographiques, les États utilisent la biométrie.

La catégorie juridique des « étrangers » est donc une « catégorie contrôlée par l'État »<sup>35</sup>, dont le fichage constitue un des outils phares.

Le fichage est également utilisé à l'encontre de ressortissants communautaires pour les identifier et les catégoriser comme soutiens aux personnes étrangères, afin soit de leur refuser des habilitations, soit de leur refuser l'entrée en France. Tel a été le cas dans plusieurs affaires concernant des personnes militantes en faveur des droits des personnes exilées, leur refusant l'entrée dans l'espace Schengen, sous couvert d'une « menace à l'ordre public »<sup>36</sup>.

---

<sup>29</sup> M. Merzouki, « Le fichier des étrangers », in *Mouvements*, n°62, 2010.

<sup>30</sup> Pierre Piazza, « [L'extension des fichiers de sécurité publique](#) », *Hermès, La Revue*, 2009/1 (n° 53), p. 67-74.

<sup>31</sup> Gérard Dubey, « [Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie](#) », in *Cahiers internationaux de sociologie*, 2008/2 (n° 125), p. 263-279. DOI : 10.3917/cis.125.0263.

<sup>32</sup> Ségolène Barbou Des Places, « [Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ?](#) », *Fichiers informatiques et sécurité publique*, Presse universitaire de Nancy, p. 183 - 221, 2013.

<sup>33</sup> La biométrie consiste à transformer une caractéristique biologique (par exemple des empreintes digitales) en une empreinte numérique.

<sup>34</sup> Ségolène Barbou Des Places, « [Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ?](#) », *Fichiers informatiques et sécurité publique*, Presse universitaire de Nancy, p. 183 - 221, 2013.

<sup>35</sup> Ségolène Barbou Des Places, « [La catégorie en droit des étrangers : une technique au service d'une politique de contrôle des étrangers](#) », in *REVUE Asylon(s)*, N°4, mai 2008, Institutionnalisation de la xénophobie en France.

<sup>36</sup> TA Nice, 4 mai 2017, n°1602391 ; TA Paris, 25 octobre 2018, n°1707798/4-1 ; TA Lille, 19 mars 2019, n°1704597.

## 2) Les fichiers comme vecteurs d'une image négative de « l'étranger »

Les lois relatives à l'immigration véhiculent une certaine image de l'« étranger ». Danièle Lochak a pu observer une évolution en France dans la vision de la personne étrangère que ces normes reflètent<sup>37</sup>. Jusque dans les années 1970, la personne étrangère était perçue sous le prisme du travailleur. Depuis a émergé la notion de « risque migratoire » et l'image que renvoie le CESEDA est celle « *d'un individu à part, d'un être dangereux, délinquant en puissance* ». Ainsi, la « menace à l'ordre public » peut être opposée aux personnes pour leur refuser l'entrée en France ou dans l'espace Schengen, du fait qu'elles sont enregistrées dans un fichier.

Les personnes étrangères sont également vues à travers les fichiers comme des personnes « fraudeuses », qui chercheraient nécessairement à « *détourner les textes ou les institutions à leur profit pour obtenir des avantages indus* »<sup>38</sup>. Nombreux sont les fichiers affichant ouvertement un objectif de « lutte contre la fraude » (AGDREF 2, OSCAR, SILCF, TES). Certains fichiers n'étant pas définis par un objectif de lutte contre la fraude véhiculent tout de même une image de « l'étranger fraudeur ».

Cette image est notamment représentée par la pratique du « shopping », contre laquelle certains fichiers européens ont été en réalité mis en œuvre, notamment les fichiers VIS et Eurodac<sup>39</sup>. Ce que cherche donc à contrer Eurodac est d'accorder à la personne le libre choix du pays européen dans lequel elle peut déposer sa demande d'asile. La personne étrangère est vue comme quelqu'un qui essaierait de « profiter » du régime d'asile qui serait « favorable » en Europe, en essayant de déposer plusieurs demandes d'asile dans différents pays de l'Union européenne pour avoir « plus de chances » de succès. Cette pratique est appelée « l'asylum shopping »<sup>40</sup>.

Dans la même logique, le VIS viserait à empêcher qu'une même personne dépose plusieurs demandes de visa simultanément dans différents pays européens pour multiplier ses chances de pouvoir venir en Europe, pratique appelée « visa shopping ». Le VIS a également pour objectif de permettre d'identifier les personnes qui se seraient maintenues sur le territoire Schengen au-delà de la durée de validité de leur visa pour pouvoir faciliter leur expulsion<sup>41</sup>. Ici encore, la personne étrangère est vue comme une personne cherchant par tout moyen à entrer dans l'espace Schengen et à s'y maintenir alors qu'elle n'y serait pas autorisée.

---

<sup>37</sup> Danièle Lochak, « [L'image de l'étranger au prisme des lois sur l'immigration](#) », Droit et Cultures - Revue internationale interdisciplinaire, CHAD (UPN), Association Droit et Cultures, L'Harmattan, 2011, Hors-série : « *Orient-Occident. Image de soi, image de l'autre* », p.125-142.

<sup>38</sup> *Ibid.*

<sup>39</sup> Ségolène Barbou Des Places, « [Fichiers et politique communautaire de l'immigration et de l'asile : une liaison fatale ?](#) », Fichiers informatiques et sécurité publique, Presse universitaire de Nancy, p. 183 - 221, 2013.

<sup>40</sup> Anafé, Note d'analyse, [L'application du règlement Dublin III aux frontières françaises - De Dublin III à Dublin IV, de la lutte contre « l'asylum-shopping » au « burden-sharing »](#), décembre 2017.

<sup>41</sup> La Cimade, [Visa Refusé, Enquête sur les pratiques des consulats de France en matière de délivrance des visas](#), juillet 2010.

## LES FICHIERS COMME OUTIL DE CONTRÔLE DES FRONTIÈRES

### Le recours aux fichiers dès la procédure de visa

#### 1) La naissance des visas

Un visa est un cachet officiel qui permet de séjourner dans un pays. Celui-ci est délivré par les autorités compétentes du pays dans lequel la personne qui en fait la demande souhaite séjourner. Souvent, la demande de visa est effectuée auprès de l'ambassade ou du consulat situé dans le pays où réside la personne.

En 1986, une vague d'attentats terroristes a frappé la France, revendiqués par le « Comité de solidarité avec les prisonniers politiques arabes et du Proche-Orient » (CSPPA), ce qui a fait émerger une volonté de contrôler davantage les frontières. Suite à l'attentat du 14 septembre sur les Champs-Élysées, le gouvernement a imposé aux personnes qui ne seraient pas issues de la Communauté européenne et de la Suisse d'obtenir un visa pour entrer sur le territoire français et a réinstauré une présence armée aux frontières. Les visas permettent à l'État d'accueil de contrôler les personnes qui entrent sur son territoire.

Au niveau européen, l'Accord Schengen est signé en 1985, suivi de la Convention de Schengen en 1990 pour l'application de l'Accord. A cette époque, les pays signataires (la France, l'Allemagne et le Benelux) décident de supprimer les contrôles des personnes à leurs frontières intérieures et, comme pour compenser, de renforcer les contrôles aux frontières extérieures. En d'autres termes, les personnes ne sont plus soumises aux contrôles lors du franchissement d'une frontière située entre deux États de l'espace Schengen.

Aujourd'hui, l'espace Schengen est composé de 26 États : 22 membres<sup>42</sup> de l'Union européenne auxquels s'ajoutent la Suisse, la Norvège, l'Islande et le Liechtenstein. Afin de favoriser la libre-circulation au sein de l'espace Schengen sans laisser une place grandissante aux migrations, une politique migratoire commune a été mise en place et notamment en matière de visas. Ainsi, plusieurs types de visas ont été mis en place :

- Le visa de court séjour permet d'entrer une ou plusieurs fois, en fonction du visa, et de circuler librement sur le territoire des différents pays de l'espace Schengen pendant une durée de 90 jours par période de six mois.
- Le visa de long séjour permet de séjourner sur le territoire Schengen pour une durée supérieure à trois mois pouvant aboutir à la délivrance d'un titre de séjour.
- Le visa mixte est un visa valable pour une durée supérieure à trois mois, n'ayant pas vocation à aboutir à la délivrance d'un titre de séjour.

Or, tous les pays tiers à l'Union européenne ne sont pas soumis à visa. Progressivement, l'obligation de visa pour les ressortissants des pays faisant partie de l'OCDE (Organisation de coopération et de développement économiques) a été supprimée. Chaque État peut unilatéralement dispenser les personnes ressortissantes d'un État tiers à l'Union européenne

---

<sup>42</sup> Belgique, Danemark, Allemagne, Estonie, Finlande, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Autriche, Pologne, Portugal, Slovénie, Slovaquie, Espagne, République tchèque, Suède.

de l'obligation de visa. Les visas ont donc été conservés uniquement pour les personnes ressortissantes des pays considérés comme « à fort risque migratoire »<sup>43</sup>.

Aussi, le règlement européen du 14 novembre 2018<sup>44</sup>, fixant l'obligation de visa pour franchir les frontières extérieures à l'espace Schengen, a modifié la liste des pays dont les ressortissants sont soumis à visa<sup>45</sup>. Désormais, 103 États sont soumis à visa et 60 États sont exemptés de cette obligation. La Bolivie et l'Équateur, auparavant non soumis à visa, ont été ajoutés à la liste des pays soumis à visa.

En revanche, ne pas être soumis à visa n'empêche pas aux personnes étrangères de devoir remplir les conditions d'entrée du pays dans lequel elles souhaitent séjourner.

En effet, les personnes étrangères, qu'elles soient soumises à visa ou pas, doivent justifier au moment du contrôle à l'entrée par la police aux frontières (PAF) qu'elles remplissent toutes les conditions d'entrée, parmi lesquelles le visa éventuel<sup>46</sup>. Le visa n'est, en effet, qu'une condition parmi d'autres pour l'entrée sur le territoire.

Les conditions d'entrée sont communes aux États membres, seules les modalités diffèrent (comme la forme de l'attestation d'accueil ou le montant des ressources)<sup>47</sup>.

Lorsque la France est le premier point d'entrée dans l'espace Schengen, c'est-à-dire que la personne transite par la France pour se rendre dans un autre État de l'espace Schengen, la PAF vérifie que les conditions d'entrée dans le pays de destination sont remplies. Dans le cas contraire, l'entrée sur le territoire sera refusée et la personne sera placée en zone d'attente.

## 2) Les fichiers consultés en amont de l'arrivée en France

Toute demande de visa est scrupuleusement étudiée par l'administration sollicitée qui consulte alors les différents fichiers auxquels elle a accès pour voir si le nom de la personne qui en fait la demande y figure et si tel est le cas, le visa pourra être refusé.

Depuis 2007, une personne qui demande un visa pour la France est automatiquement inscrite dans le fichier national VISABIO. Ce fichier a été mis en place dans le but d'effectuer un contrôle accru des demandes de visa et de lutter contre la fraude. Il comporte les images numérisées de la photographie et des empreintes digitales des dix doigts. Il est également complété après l'obtention du visa par les dates d'entrée et de sortie du territoire Schengen.

A titre d'exemple, VISABIO peut être consulté pour savoir s'il s'agit d'une première demande de visa et si non, quelle a été l'issue des demandes antérieures. Il sert aussi à vérifier si la personne a déjà demandé un visa sous une autre identité.

Ce fichier accède aux données du fichier RMV 2<sup>48</sup>, permettant un échange entre États des

---

<sup>43</sup> La notion de « risque migratoire » est une notion clef du contrôle des frontières, sans réel cadre légal, qui conduit nécessairement à des décisions discriminatoires, voire arbitraires. Et le terme « risque » renvoie directement à la notion de menace, ce qui participe à la criminalisation des personnes migrantes.

<sup>44</sup> Règlement modifiant le règlement (CE) n°539/2001 du Conseil fixant la liste des pays tiers dont les ressortissants sont soumis à l'obligation de visa pour franchir les frontières extérieures des États membres et la liste de ceux dont les ressortissants sont exemptés de cette obligation.

<sup>45</sup> Anafé, [Liste des pays non soumis à visa, des pays soumis à visa, des accords de facilitations de délivrance des visas et des pays soumis à visa de transit aéroportuaire](#).

<sup>46</sup> Anafé, [Conditions d'entrée en France et dans l'espace Schengen](#).

<sup>47</sup> Anafé, [Conditions d'entrée dans l'espace Schengen en fonction du pays de destination](#).

<sup>48</sup> Réseau mondial visa 2.

informations relatives aux demandes de visas. Ainsi, les États renseignent les données dans un fichier et n'importe quel autre État peut vérifier les différentes demandes de visa déposées pour entrer dans l'espace Schengen, mais aussi les dates d'entrée et de sortie correspondant aux visas délivrés.

D'autres interconnexions existent entre les fichiers qui se nourrissent les uns des autres. En ce sens, VISABIO et RMV 2 sont tous deux interconnectés avec le fichier VIS II (Visa information system). Ce dernier est, lui aussi, consulté dès lors qu'une personne demande un visa pour venir en France ou dans l'espace Schengen.

L'objectif de ce fichier serait d'examiner les demandes de visa de court séjour afin de lutter contre le « visa shopping », c'est-à-dire éviter que des personnes fassent plusieurs demandes de visa simultanées auprès de plusieurs services consulaires. Il permet également d'identifier les personnes restées sur le territoire européen au-delà de la durée de validité de leur visa.

D'autres fichiers sont encore consultés dans le cadre de l'examen d'une demande de visa. C'est notamment le cas du fichier AGDREF 2 qui répertorie depuis 2011 toutes les personnes étrangères ayant entrepris des démarches relatives à l'entrée ou au séjour en France, et ce depuis la France ou l'étranger. Son objectif est de lutter contre l'entrée et le séjour dits irréguliers mais aussi contre la fraude documentaire.

Le fichier GIPI (Gestion informatisée des procédures d'immigration) est lui aussi pris en compte dès la procédure de visa. Il contient des informations relatives aux personnes à qui l'entrée dans l'espace Schengen a été refusée lors du franchissement de la frontière. Autrement dit, ce fichier contient toutes les informations relatives au maintien en zone d'attente, allant du motif du refus d'entrée à la sortie en passant par la présentation devant les juridictions compétentes.

Enfin, les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique sont regroupées dans le FPR (Fichier des personnes recherchées). Ce fichier vise à faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives. Il contient 21 sous-fichiers en fonction du fondement juridique de la recherche dont le fichier S relatif à la sûreté de l'État. L'administration consulte ce fichier avant l'attribution d'un visa au motif qu'une personne renseignée dans ce fichier constituerait une menace à l'ordre public.

En France, depuis le 29 juin 2019, tous les passeports délivrés sont des passeports biométriques, c'est-à-dire qu'ils comportent une puce qui stocke la photographie numérisée de la personne ainsi que ses empreintes digitales. Ces données seront donc enregistrées dans les fichiers VISABIO et VIS II dès lors que le titulaire d'un passeport biométrique effectuera une demande de visa.

Mais l'utilisation de la biométrie s'accroît s'agissant des contrôles effectués sur les personnes en amont de leur venue. En effet, si les passeports biométriques sont de plus en plus répandus à travers le monde, ils sont également de plus en plus considérés comme une condition à l'entrée sur le territoire, comme une garantie en quelque sorte de la bonne foi de la personne. Lorsqu'on regarde de plus près la liste des pays dont les ressortissants ne sont pas soumis à l'obligation de visa, il apparaît que le passeport biométrique peut être une



condition à cette exemption<sup>49</sup>. Ainsi, les personnes ressortissantes des Émirats Arabes Unis, des Îles Marshall, du Monténégro ou encore de la Dominique ne sont pas soumis à visa seulement si elles ont un passeport biométrique.

Des visas additionnels peuvent être demandés pour transiter par un aéroport situé sur le territoire Schengen. Il s'agit des visas de transit et des visas de transit aéroportuaire (VTA)<sup>50</sup>. Selon la nationalité, ces visas peuvent être exigés dans le cadre d'une escale ayant lieu dans un aéroport situé en Europe.

Le visa de transit est nécessaire lorsque le ressortissant d'un État hors Schengen voyage vers un autre État également situé hors de l'espace Schengen mais doit, pour cela, passer par la France. Ce visa lui permettra d'entrer sur le territoire quelques jours pour effectuer cette traversée.

A l'inverse, le VTA correspond à « l'autorisation à laquelle sont soumis les ressortissants de certains pays tiers par exception au principe de libre transit posé par l'annexe 9 de la convention de Chicago relative à l'aviation civile internationale, pour transiter par la zone internationale des États membres ». Concrètement, il permet de contrôler les personnes pouvant faire une escale, quand bien même ces personnes resteraient dans la zone internationale de l'aéroport sans même entrer sur le territoire Schengen.

Ces deux types de visas de transit sont complémentaires des visas dits classiques. Ils imposent de faire une demande additionnelle et constituent un contrôle supplémentaire. L'examen de ces demandes de visa amène l'administration française à consulter de nouveau les fichiers pour vérifier l'inscription ou non de la personne qui en fait la demande.

## L'utilisation des fichiers aux frontières extérieures françaises

### 1) L'usage des fichiers par les services administratifs et de police...

#### ... A l'arrivée aux frontières et pendant le maintien en zone d'attente

Que les personnes soient soumises ou non à l'obligation de visa, elles sont contrôlées par la police aux frontières à leur arrivée en France ou dans le premier pays d'entrée sur le territoire Schengen.

Deux types de contrôles sont mis en place par la police aux frontières lors d'une arrivée dans un aéroport : celui se déroulant en porte d'avion appelé le « contrôle passerelle » et celui se déroulant aux aubettes (box vitrés) où le passage est obligatoire pour quitter la zone internationale de l'aéroport.

Les contrôles passerelles sont organisés et effectués de manière non systématique et le fichier API-PNR (Advance passenger information - passenger name record) peut être utilisé à

---

<sup>49</sup> Anafé, [Liste des pays non soumis à visa, des pays soumis à visa, des accords de facilitations de délivrance des visas et des pays soumis à visa de transit aéroportuaire](#).

<sup>50</sup> Note de l'Anafé, « [Les visas de transit aéroportuaire imposés par la France : État des lieux et enjeux](#) », juillet 2017.

L'Union européenne a dressé une liste commune des pays dont les ressortissants sont soumis à VTA comportant, entre autres, l'Afghanistan, le Sri Lanka et la Somalie. Néanmoins, chaque État de l'espace Schengen dispose de la possibilité d'élargir cette liste, ce qu'a fait la France avec 17 États supplémentaires. A titre d'exemple, sont soumis à VTA français les ressortissants de la Syrie, du Sénégal et de Cuba.

ce stade puisqu'y sont renseignées les données de réservations ainsi que les données d'enregistrement et d'embarquement de tous les passagers Ce fichier est interconnecté, entre autres, avec les fichiers FPR, SIS II et celui des documents de voyage volés et perdus d'Interpol.

Les contrôles passerelles peuvent être mis en place dans le cadre de la recherche d'une personne précisément identifiée mais également de manière aléatoire (notamment sur les vols considérés comme à « risque migratoire »).

A l'inverse, les contrôles en aubettes sont systématiques pour toutes les personnes débarquant d'un avion. Lors de ce contrôle, le passeport de la personne est scanné dans le boîtier QUOVADIS qui affiche sur l'ordinateur des informations relatives à la personne, grossit sa photographie et alerte l'agent de police si la personne est inscrite dans des fichiers comme les fichiers VISABIO, SIS II, TAJ, RMV2, FPR, Interpol ou encore le FAED, qui est le fichier automatisé des empreintes digitales des personnes mises en cause dans une procédure criminelle ou délictuelle afin de faciliter leur poursuite, leur instruction et leur jugement. Ce fichier est alimenté par les services de police judiciaire français et étrangers. Dans la même idée, le fichier FNAEG contient, quant à lui, des empreintes génétiques afin de faciliter l'identification et la recherche des auteurs d'infractions et des personnes disparues.

Ainsi, à l'arrivée des personnes étrangères en France, au moins huit fichiers nationaux, européens ou internationaux sont systématiquement consultés.

Enfin, lorsque l'entrée est refusée à une personne, le logiciel GIPI sert à « *faciliter la gestion des procédures de non-admission des étrangers qui ne remplissent pas les conditions d'entrée dans l'espace de libre circulation des personnes entre les États signataires de l'accord de Schengen [...]* ». Il délivre les différents documents de notification de refus d'entrée sur le territoire et s'apparente donc à un fichier qui regroupe les informations des personnes non admises sur le territoire.

### **... A la fin du maintien en zone d'attente**

Les fichiers ne sont pas uniquement pris en compte dans le cadre de la procédure de visa et de l'arrivée dans l'espace Schengen, mais également lors de la sortie de la zone d'attente.

Si le maintien en zone d'attente peut prendre fin par la libération ou le réacheminement de la personne, le placement en garde à vue est aussi un motif de sortie. Ce dernier peut être décidé lorsque la personne refuse d'embarquer ou de communiquer les informations nécessaires à son renvoi. Au terme de la garde à vue, le procureur peut décider d'engager ou non des poursuites judiciaires contre la personne.

Dans ce contexte, différents fichiers de police (comme AGEDREF 2, FPR, RMV 2 ou VISABIO) sont consultés par le procureur ou la préfecture. C'est également le cas du fichier TAJ qui regroupe des données recueillies par la police, la gendarmerie nationale et les agents des douanes judiciaires et est utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et administratives (enquêtes préalables à certains emplois publics ou sensibles). Le fichier TAJ est différent du casier judiciaire en ce qu'il recueille également les rappels à la loi qui ne sont pas présents sur un casier judiciaire.

D'autres fichiers peuvent être vérifiés comme le fichier GESTEL (Gestion de l'éloignement) qui assure la gestion de la mise en œuvre opérationnelle, matérielle et logistique des mesures d'éloignement du territoire et à assurer le suivi des procédures. Il sera alors possible de vérifier si une personne sortant de zone d'attente a déjà fait l'objet d'une mesure

d'éloignement, ce qui pourrait être un motif pour prendre une obligation de quitter le territoire français (OQTF) à son encontre. Cette mesure peut entraîner un placement immédiat en centre de rétention administrative<sup>51</sup>.

Il est possible pour la police de prendre les empreintes digitales ou de recueillir l'ADN des personnes gardées à vues. Ces échantillons seront respectivement répertoriés dans le fichier FAED ou FNAEG<sup>52</sup>.

Enfin, dans le cadre de ses permanences juridiques, l'Anafé a eu à connaître la situation d'une personne qui était arrivée en zone d'attente avec des faux documents puis réacheminée, et lors d'un second placement en zone d'attente quelques semaines après, elle a appris qu'elle était désormais signalée dans le fichier SIS II. N'ayant jamais voyagé en dehors de son pays auparavant, cette inscription dans le fichier SIS II semblerait donc directement liée au premier refus d'entrée motivé par la détention de faux documents. Une telle pratique serait donc particulièrement attentatoire au droit d'asile pour les personnes en quête de protection et qui ne seraient parvenues à fuir qu'avec des faux documents.

### **Le cas particulier des demandes d'asile**

Le règlement européen « Dublin III »<sup>53</sup> prévoit qu'un seul État membre de l'Union européenne peut examiner une demande d'asile et dresse une liste de critères afin de déterminer le pays responsable de l'examen de cette demande. Les fichiers sont donc consultés pour mettre en œuvre la procédure prévue par le règlement.

L'article 12 du règlement « Dublin III » indique que l'examen de la demande d'asile d'une personne en possession d'un titre de séjour ou d'un visa doit être effectué dans le pays lui ayant délivré ledit titre de séjour ou visa, quand bien même il aurait effectué sa demande d'asile dans un autre État. Dans ce cadre, l'administration utilise les fichiers VISABIO et VIS II. S'il apparaît que la personne a un visa ou un titre de séjour délivré par un autre État membre de l'Union européenne, la personne demandeuse d'asile pourra être transférée dans cet autre État.

Il en va de même pour les personnes entrées par un autre État membre ou qui ont déjà déposé une demande d'asile dans un autre État. Elles pourront être transférées depuis la zone d'attente vers cet État dès lors qu'elles apparaissent dans le fichier EURODAC (EU Biometric data base). Il s'agit d'un système d'information à grande échelle contenant les empreintes digitales des demandeurs d'asile ou de protection subsidiaire et des personnes migrantes considérées comme en situation irrégulière sur le territoire de l'UE.

Le règlement prévoit également qu'un demandeur d'asile puisse être transféré dans un État membre où un ou des membres de sa famille sont en procédure asile ou bénéficient du statut de réfugié. Le fichier EURODAC peut donc être consulté à cet effet.

---

<sup>51</sup> Depuis janvier 2018, la préfecture de Seine-Saint-Denis prend régulièrement des OQTF fondées sur différents motifs avec placement immédiat en CRA à l'encontre de personnes qui avaient été placées en garde à vue à l'issue de leur maintien en zone d'attente de l'aéroport de Roissy Charles de Gaulle.

<sup>52</sup> « [Gardé-e-s à vue du 29 novembre 2015 : que faire ?](#) » publié le 13 décembre 2015 sur le site *Paris Luttes Infos*.

<sup>53</sup> Règlement (UE) no 604/2013 du Parlement européen et du Conseil du 26 juin 2013 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande de protection internationale introduite dans l'un des États membres par un ressortissant de pays tiers ou un apatride.

Cependant, il est impossible de renvoyer un demandeur d'asile vers un autre État membre si des défaillances systémiques en termes de protection sont connues dans cet État et qui entraîneraient un risque de traitement inhumain et dégradant. Si après une recherche, aucun autre pays ne peut être considéré comme responsable selon les critères établis par le règlement, l'État dans lequel la demande a été faite en sera en charge.

S'agissant de la sortie de zone d'attente, toutes les personnes admises sur le territoire au titre de l'asile, c'est-à-dire sur décision du ministère de l'intérieur prise après avis de l'OFPRA, sont inscrites dans EURODAC mais également dans les fichiers nationaux DNA et INEREC. Le fichier DNA correspond au Dispositif national d'accueil des personnes demandeuses d'asile qui a pour objectif de vérifier les conditions d'accueil en France, aussi bien en termes d'accompagnement administratif que d'hébergement. Quant au fichier INEREC, il vise à aider à la gestion des demandes d'asile par l'OFPRA, en permettant l'échange d'informations avec les préfetures et le ministère de l'intérieur sur la situation des demandeurs d'asile.

## 2) La prise en compte des fichiers par les juridictions

Selon l'article L. 213-1 du CESEDA, « *l'accès au territoire français peut être refusé à tout étranger dont la présence constituerait une menace pour l'ordre public ou qui fait l'objet soit d'une peine d'interdiction judiciaire du territoire, soit d'un arrêté d'expulsion, soit d'un arrêté de reconduite à la frontière pris moins de trois ans auparavant en application de l'article L.533-1, soit d'une interdiction de retour sur le territoire français, soit d'une interdiction administrative du territoire* ».

Lors de ses permanences juridiques, l'Anafé constate que des personnes se voient refuser l'entrée sur le territoire du fait de leur inscription dans un fichier national ou européen. Le plus fréquemment, ces personnes font l'objet d'une fiche SIS II qui leur interdit l'accès à l'ensemble de l'espace Schengen pour une durée déterminée mais possiblement reconductible. Lorsque les personnes maintenues en zone d'attente sont présentées devant le juge judiciaire ou le juge administratif<sup>54</sup>, les fichiers jouent un rôle important dans l'examen de la situation qui sera faite par le magistrat et partant, dans la décision de mettre fin ou non à la privation de liberté.

Dans l'hypothèse où les personnes sont toujours en zone d'attente au bout de 4 jours, elles sont présentées devant le juge des libertés et de la détention (JLD) une à deux fois selon la durée de leur maintien<sup>55</sup>. Il leur est possible de présenter des garanties (appelées garanties de représentation) afin d'être autorisées à entrer sur le territoire. Or, en général, le JLD prolonge le maintien en zone d'attente des personnes fichées SIS quand bien même elles présenteraient ces garanties.

Par ailleurs, si le juge administratif est saisi, il doit opérer un contrôle de la légalité de la

---

<sup>54</sup> Pour plus d'informations sur la procédure en zone d'attente, voir le [support de formation](#) disponible sur le site de l'Anafé.

<sup>55</sup> Le contrôle du respect des droits et des conditions de maintien en zone d'attente est dévolu au juge des libertés et de la détention, juge judiciaire, gardien des libertés individuelles, qui intervient au bout de 4 jours. Au vu de la durée maximum de maintien (20 jours) et de la durée moyenne de maintien (en 2017 : 4,21 jours à Roissy, 72 heures à Orly et moins de 24 heures dans les autres zones d'attente), l'intervention du juge des libertés et de la détention arrive tardivement et a pour conséquence que la majorité des personnes maintenues ne rencontreront jamais le JLD.

décision de refus d'entrée. Ainsi, le tribunal administratif de Nice<sup>56</sup> a précisé qu'un refus d'entrée se fondant sur une inscription dans un fichier doit faire l'objet d'une « *décision spécialement motivée* ». Dans le cas contraire, il convient d'annuler le refus d'entrée. Une telle annulation est également possible s'agissant des risques de trouble à l'ordre public. Pour justifier un refus d'entrée, la menace que risque de représenter la personne doit être réelle, actuelle et suffisamment grave<sup>57</sup>.

La possibilité de contrôler la légalité d'un refus d'entrée sur le territoire par le juge administratif est d'autant plus importante que les fichiers ne sont pas nécessairement fiables.

## Entre les mailles des fichiers : les failles

Les fichiers peuvent être attentatoires aux libertés et droits fondamentaux des personnes en ce qu'ils peuvent notamment impacter le droit au respect de la vie privée et familiale<sup>58</sup>, la liberté d'aller et venir<sup>59</sup> ou encore l'intérêt supérieur de l'enfant<sup>60</sup>.

De plus, se pose la question du respect de la Réglementation générale pour la protection des données personnelles au sein de l'Union européenne. Pour se faire, le Parlement européen et le Conseil ont décidé d'adopter un Règlement en mai 2019<sup>61</sup> qui prévoit le partage des données et l'interconnexion des différents systèmes d'informations de l'Union européenne tout en protégeant les données personnelles par le biais d'un « *portail de recherche européen (ESP), un service partagé d'établissement de correspondances biométriques (BMS partagé), un répertoire commun de données d'identité (CIR) et un détecteur d'identités multiples (MID)* ».

Mais en raison des nombreuses failles révélées en pratique par l'utilisation des fichiers, il semble raisonnable de penser que ce système présentera des dysfonctionnements.

Parmi les failles les plus fréquentes, se trouvent notamment la fiabilité de la biométrie, l'actualisation des fichiers et l'information des personnes de leur inscription dans un fichier.

---

<sup>56</sup> TA Nice, 6 avril 2017, n°1602391.

<sup>57</sup> TA Paris, 11 octobre 2018, n°1707798/4-1.

<sup>58</sup> Article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales :

« *Droit au respect de la vie privée et familiale*

1. *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

2. *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

<sup>59</sup> La liberté d'aller et venir constitue une liberté fondamentale au sens des dispositions de l'article L. 521-2 du code de justice administrative (CC, 12 janvier 1979, N°79-107 DC ; CE, 9 janvier 2001, n° 228928 ; CE, 26 juin 2006, n° 294505 et 294506).

<sup>60</sup> Article 3 de la convention internationale des droits de l'enfant :

« 1. *Dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale.*

2. *Les Etats parties s'engagent à assurer à l'enfant la protection et les soins nécessaires à son bien-être, compte tenu des droits et des devoirs de ses parents, de ses tuteurs ou des autres personnes légalement responsables de lui, et ils prennent à cette fin toutes les mesures législatives et administratives appropriées. [...] »*

<sup>61</sup> Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) no 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil.

**S’agissant de la biométrie**, y recourir serait considéré comme un gage de vérité, une sorte de garantie inébranlable.

Ainsi, l’identité d’une personne est réduite à ses caractéristiques biologiques par l’administration. Or, la biométrie n’est certainement pas aussi fiable que la certitude avec laquelle elle est pourtant utilisée lors des contrôles aux frontières. Comme le soulève Pierre Piazza, « *présentée comme infaillible, la biométrie occasionne des taux d’erreurs non négligeables en raison de l’extrême précision qu’impliquent la captation, le traitement et la lecture des données corporelles* »<sup>62</sup>. La marge d’erreur de la biométrie ne semble pas être prise en compte par l’administration lors des contrôles qu’ils aient lieu en amont ou lors de l’arrivée à la frontière.

A titre d’exemple, le tribunal administratif de Nantes a annulé des arrêtés de transfert et portant assignation à résidence pris en raison de l’inscription d’une personne dans le fichier EURODAC, les empreintes digitales de tous les doigts n’ayant pas été prises par la France alors qu’elles avaient toutes été enregistrées en Espagne<sup>63</sup> : il ne peut pas y avoir de certitude quant à l’identité de la personne car il est nécessaire que les empreintes digitales enregistrées dans le fichier EURODAC soient strictement identiques.

**L’absence d’actualisation systématique et fiable** des fichiers montre également les limites de leur utilisation. Les fichiers ne sont effectivement pas toujours correctement complétés, c’est ce qu’a affirmé un fonctionnaire de la sous-direction de la police technique et scientifique en 2006 à propos du FNAEG<sup>64</sup>.

Cela peut s’expliquer de plusieurs manières. Dans un premier temps, la multiplication des fichiers implique de saisir de plus en plus de données pouvant alors mener à des renseignements incomplets, différés ou erronés. En ce sens, le tribunal administratif de Paris a annulé un arrêté de transfert vers l’Espagne car les empreintes digitales d’une personne étrangère avaient été enregistrées dans le fichier EURODAC par l’Espagne au mois d’octobre alors que celui-ci se trouvait en France depuis le mois de septembre<sup>65</sup>.

Ensuite, les fichiers ne sont pas toujours actualisés et, quand ils le sont, cela ne se fait pas forcément instantanément. Pour pouvoir actualiser un fichier, il faut être en possession de données supplémentaires sur la personne et être en mesure de les renseigner. Or, ce n’est pas tout le temps le cas alors que les situations personnelles et individuelles des personnes, elles, évoluent. Cela amène donc à une péremption des fichiers qui implique que des personnes peuvent être dans des fichiers alors qu’elles n’ont plus de raison d’y figurer. Cela peut être dû à une décision qui justifiait leur inscription sur un fichier qui a expiré. Par exemple, elles peuvent donc être interdites de visa ou d’entrée sur le territoire pour un motif qui n’est plus réel et actuel et qui n’est donc plus valable.

De plus, l’accès aux fichiers par les personnes qui font l’objet d’une fiche est souvent complexe. L’accès à sa fiche est le seul moyen pour une personne de vérifier les informations qui y sont renseignées et de faire rectifier les mentions erronées ou périmées. La procédure d’accès est censée être simple : le plus souvent il faut envoyer une lettre ainsi qu’une copie de sa pièce d’identité à la Commission nationale de l’informatique et des libertés (CNIL) ou à l’autorité compétente. Or, il est fréquent qu’après plusieurs démarches l’accès à la fiche soit

---

<sup>62</sup> Pierre Piazza, « [L’extension des fichiers de sécurité publique](#) », *Hermès, La Revue*, 2009/1 (n° 53).

<sup>63</sup> TA Nantes, 9 avril 2019, n° 1903480.

<sup>64</sup> Pierre Piazza, « [L’extension des fichiers de sécurité publique](#) », *Hermès, La Revue*, 2009/1 (n° 53).

<sup>65</sup> TA Paris, 3 avril 2018, n° 1804203/8.

refusé pour des raisons de sécurité nationale (motif qui peut regrouper un grand nombre d'hypothèses plus ou moins fondées). En pareil cas, les fichiers ne peuvent être actualisés que par les autorités, ce qui ne permet pas de lutter efficacement contre les fichiers périmés ou non actualisés.

**La connaissance de son inscription dans un fichier** est un autre problème. Il arrive régulièrement que les personnes suivies par les permanences de l'Anafé se soient vues refuser l'entrée sur le territoire en raison d'une fiche dont elles n'avaient pas connaissance ou bien dont elles n'en connaissaient pas les modalités. Ces personnes apprennent cela à la frontière. Certaines sont également au fait de leur fiche mais ne savent pas qu'elle s'applique à l'intégralité du territoire Schengen (exemple du fichier SIS II) ou qu'elle est toujours valable. Cela met en lumière un manque d'information qui ne permet donc pas aux personnes visées de contester ou de faire rectifier les informations collectées. La méconnaissance de l'inscription dans un fichier peut aussi se traduire différemment. L'Anafé a pu suivre des personnes dont la fiche SIS II avait expiré mais avait été renouvelée sans qu'elles en soient informées. Ainsi, certaines attendent la date d'expiration d'une fiche avant de venir de nouveau en Europe et lorsqu'elles arrivent elles se font refuser l'entrée pour les mêmes motifs car ladite fiche a été reconduite.

Enfin, l'objet de certains fichiers est dévoyé. Dans le cadre de la rétention administrative, la cour d'appel de Montpellier a infirmé des décisions du juge des libertés et de la détention qui prolongeaient la rétention administrative de personnes car le fichier FAED avait été consulté par une personne qui n'y était pas habilitée ou dont habilitation ne pouvait pas être vérifiée<sup>66</sup>.

## La banalisation du fichage lors des contrôles aux frontières intérieures

Les contrôles ne sont pas uniquement effectués aux frontières extérieures, mais aussi dans certains cas aux frontières intérieures de l'espace Schengen, comme c'est le cas depuis 2015 suite au rétablissement des contrôles aux frontières internes<sup>67</sup>.

Il existe alors différents points de contrôles. Tout d'abord, il y a les points de passage autorisés (PPA) où sont effectués des contrôles fixes et systématiques 24 heures sur 24. Ces PPA ont été listés et communiqués à la Commission européenne en décembre 2015<sup>68</sup>. Ensuite, d'autres zones de contrôles sont mises en place pour des contrôles ne pouvant, en théorie, pas excéder 12 heures<sup>69</sup>. Or, en pratique, aucune précision n'est apportée par la loi, notamment sur la durée exigée entre deux contrôles, ce qui peut rendre les contrôles continus. De plus, l'étendue de ces contrôles diffère en fonction des différents textes qui les prévoient. Si le code frontières Schengen prévoit une borne de 20 kms au-delà de la frontière, la réforme du CESEDA adoptée septembre 2018 instaure quant à elle une borne de 10 kms à partir de la frontière<sup>70</sup>. Aussi, la loi de 2017 renforçant la sécurité intérieure ajoute

---

<sup>66</sup> CA Montpellier, 8 avril 2019, n° 2019-174 et CA Montpellier, 12 avril 2019, n° 2019-183.

<sup>67</sup> Anafé, Note d'analyse : Rétablissement des contrôles aux frontières internes et état d'urgence - Conséquences en zone d'attente, mai 2017.

<sup>68</sup> La [liste des PPA](#) est disponible sur le site du Conseil de l'Union européenne.

<sup>69</sup> Auparavant, 6 heures portées à 12 heures depuis la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme.

<sup>70</sup> Loi n° 2018-778 du 10 septembre 2018 pour une immigration maîtrisée, un droit d'asile effectif et une intégration réussie.

de nouvelles zones de contrôles autour de certains ports et gares sur le territoire ainsi qu'autour de certains péages.

Les ressortissants communautaires au même titre que les ressortissants d'États tiers à l'espace Schengen peuvent donc être soumis à des contrôles sur leur identité et les motifs de leur séjour dès lors qu'ils franchissent une frontière de la France, même terrestre. Toutefois, ces contrôles sont majoritairement réalisés au faciès sur des personnes dites « d'apparence migrante »<sup>71</sup>.

Particulièrement à la frontière franco-italienne, si les personnes interceptées ne peuvent justifier de ces raisons ou de leur identité, elles font l'objet d'un refus d'entrée sans examen individuel de leur situation administrative. Cela est renforcé par le défaut d'interprètes pour assurer la traduction entre les agents de la police aux frontières et les personnes non admises lors de la notification des droits et de la procédure. Concrètement, les personnes sont emmenées au poste de la PAF qui met en place une procédure expéditive : il peut s'écouler seulement quelques minutes entre le refus d'entrée et le refoulement. Outre le défaut d'interprétariat, les droits ne sont pas notifiés aux personnes non admises.

Auparavant, le refus d'entrée était établi pour absence de documents mais depuis le début de l'année 2019, l'Anafé constate que des refus d'entrée sont aussi de plus en plus fondés sur le risque de trouble à l'ordre public. Cette pratique montre que le rétablissement des contrôles aux frontières, annoncé pour lutter contre le terrorisme, cherche davantage à lutter contre l'immigration. En effet, le caractère expéditif de la procédure de refus d'entrée sur le territoire ne laisse pas le temps de vérifier que la personne non admise constituerait une véritable menace à l'ordre public. Surtout, le renforcement des contrôles aux frontières internes est concentré au niveau des passages de personnes en migration, c'est à dire à la frontière franco-italienne et à la frontière franco-espagnole. Le rétablissement des contrôles aux frontières internes sert donc de prétexte aux contrôles ciblés pour empêcher l'entrée en France de personnes en exil et en provenance d'Italie et d'Espagne et le motif de menace à l'ordre public servirait alors de justification.

La gare de Modane dispose d'une zone d'attente. C'est l'argument sur lequel se fonde la PAF pour justifier la consultation des différents fichiers à l'arrivée des personnes en France mais également pendant et jusqu'à la fin du maintien en zone d'attente.

Un rapport du CGLPL faisant suite à une visite réalisée courant septembre 2017<sup>72</sup> indique la présence d'un registre (appelé Film ESI Menton) à Menton, lequel serait alimenté par des informations relatives aux entrées et sorties du poste de police. Ce registre comporte la durée s'écoulant entre l'interpellation et le refoulement en précisant les horaires de chaque étape de la procédure mais également des informations relatives à l'identité des personnes. Cependant, ce fichier comporte également des failles car des informations sont souvent manquantes ou fausses.

Si au niveau des autres frontières intérieures, les fichiers de police ne seraient pas systématiquement consultés (au vu notamment de la procédure expéditive mise en place), l'Anafé ne dispose pas d'informations sur les pratiques pour l'ensemble des points de contrôles aux frontières franco-italienne et franco-espagnole.

---

<sup>71</sup> Anafé, [Persona non grata - Conséquences des politiques sécuritaires et migratoires à la frontière franco-italienne, Rapport d'observations 2017-2018](#), février 2019, p. 19 et s.

<sup>72</sup> CGLPL, [Rapport de la deuxième visite des services de la police aux frontières de Menton \(Alpes-Maritimes\)](#), septembre 2017.



## LE FRANCHISSEMENT DES FRONTIÈRES PAR LES CITOYENS EUROPÉENS : LES DERIVES DU FICHAGE

Le franchissement des frontières n'est pas une épreuve réservée aux personnes étrangères à l'Union européenne.

A titre d'exemple, un militant français fiché S a témoigné de son passage par le contrôle de police à l'aéroport de Beauvais en 2018<sup>73</sup>.

Alors qu'il prenait l'avion pour la première fois, il a eu à connaître de comment il était perçu par le gouvernement en raison de son fichage. Après avoir passé le contrôle de la PAF sans difficulté et alors qu'il se dirigeait vers l'embarquement, il s'est rendu compte que sur l'ordinateur du policier son visage était affiché, une photo prise un mois auparavant pour son passeport et accolé à son nom, en gros et en rouge, la signalétique suivante : « *Individu dangereux* » et une indication à l'attention des forces de la police : « *Ne pas attirer l'attention* ». Malgré tout, le policier est sorti de son poste et a évoqué avec lui - devant les autres passagers - sa fiche S. Alors que le militant était au courant depuis 8 ans de son fichage, il a compris, au vu de ce que lui sous-entendait le policier et de la photo récente, que sa fiche était non seulement « à jour » mais évoquait ses actions actuelles pour lesquelles il n'avait pas été inquiété. A noter que le policier lui a précisé « *Bon ceci dit, on ne va pas vous empêcher de partir pour ça* ». Alors que le militant se renseignait pour connaître les démarches afin de faire retirer sa fiche, le policier lui a indiqué qu'au vu de son contenu, il n'obtiendrait pas gain de cause<sup>74</sup>. Ce type de fichage permet une forme d'intimidation et de surveillance constante.

Le fichage des militants, dans une visée de surveillance accrue et de contrôle des activités et des mouvements sociaux, doit être regardé au prisme de la réglementation sur les fichiers et de celle sur la protection des données personnelles.

A cet égard, la Cour européenne des droits de l'homme a jugé que la collecte et la conservation par la police de données concernant un militant jamais condamné dans un fichier relatif à l'« extrémisme » ne respectait pas l'obligation de protéger sa vie privée, en violation de l'article 8 de la Convention. En effet, dans un arrêt du 24 janvier 2019, la Cour a estimé que la décision de conserver des informations sur l'intéressé n'a pas tenu compte de la protection renforcée applicable aux données révélant les opinions politiques d'une personne. Par conséquent, elle a rejeté l'argument du gouvernement britannique selon lequel il serait trop difficile de réexaminer et d'effacer toutes les données concernant le requérant en ce que la base de données relative à l'extrémisme ne serait pas automatisée<sup>75</sup>.

La surveillance des mobilisations politiques et sociales n'est pas nouvelle mais elle est de plus en plus favorisée par le développement des nouvelles technologies et des fichiers. Les

---

<sup>73</sup> « *Individu dangereux* » : ce qu'un passage à l'aéroport apprend sur le fichage des militants », publié le 7 octobre 2018 sur le site [Paris Luttes Info](#).

<sup>74</sup> Une demande de retrait de la fiche S est une procédure administrative soumise à enquête sur les actions, les pratiques et les contacts de la personne qui en demande le retrait. Le [journaliste Gaspard Glanz](#) a d'ailleurs témoigné de sa propre expérience. De plus, toute fiche S doit être renouvelée tous les ans, « *Elle peut être renouvelée si la poursuite de la surveillance paraît nécessaire.* » selon le site gouvernemental [Stop-Djihadisme](#).

<sup>75</sup> CEDH, 1ère section, 24 janvier 2019, n° 43514/15, [Catt c/ Royaume-Uni](#).

informations ainsi recueillies et partagées sur les personnes militantes deviennent une étiquette « à surveiller » dont il est particulièrement difficile de se défaire et qui peut facilement glisser vers le « risque de menace à l'ordre public ».

Face au durcissement croissant des politiques migratoires toujours plus répressives, des personnes et des associations travaillent pour restaurer la solidarité et la fraternité, comme à la frontière franco-italienne. La lutte contre l'immigration ne se limite plus aux personnes étrangères mais elle s'étend à leurs soutiens. Certaines de ces personnes militantes pour le respect des droits – et de plus en plus – font l'objet de pressions quotidiennes, de poursuites judiciaires et de condamnations des personnes solidaires<sup>76</sup>. Partout en Europe, de plus en plus de militants sont surveillés, fichés, subissent des pressions, sont convoqués à des auditions, placés en garde à vue, poursuivis, ou condamnés pour ce que l'on appelle le « délit de solidarité »<sup>77</sup>. Le prétexte sécuritaire est utilisé pour entraver les déplacements et l'action des personnes militantes. Le contexte actuel est donc celui d'une criminalisation croissante.

Récemment, la justice française a eu à se prononcer sur la légalité de refus d'entrée sur le territoire français opposés par la police aux frontières française à des ressortissants européens, au prétexte d'une menace à l'ordre public.

Tout d'abord, en 2017, le tribunal administratif de Nice a annulé<sup>78</sup> un refus d'entrée, pris à l'aéroport de Nice à l'encontre d'un ressortissant italien militant notamment à la frontière franco-italienne, au motif que « *le refus d'entrée sur le territoire français doit faire l'objet d'une décision spécialement motivée [...]. La décision contestée [...] se borne toutefois à indiquer que M. X « est signalé aux fins de non admission », d'une part, et « dans le fichier national (mesures d'expulsion, d'éloignement, d'interdiction du territoire, menace de trouble à l'ordre public) », d'autre part, sans mentionner aucune circonstance de fait* ».

Ensuite, la police aux frontières française, en poste à la gare internationale de Saint-Pancras (à Londres), a opposé un refus d'entrée à un ressortissant irlandais au motif d'une prétendue inscription dans un « fichier national », une supposée appartenance à la mouvance « No border » et, surtout, différents « signalements », liés à la participation de Monsieur à des manifestations de soutien aux personnes exilées. Un recours a été déposé faisant valoir que la décision avait été prise en violation du principe de la liberté de circulation des citoyens européens dans l'Union – qui ne peut céder qu'en présence d'une « menace réelle et actuelle à un intérêt fondamental de la société » –, et que la preuve du risque de menace à l'ordre public n'était pas rapportée. Pour se justifier, le ministère de l'intérieur a produit une « note blanche »<sup>79</sup> et tenté de soutenir que Monsieur était susceptible de se livrer à des actions violentes, de sorte que sa venue en France comportait un risque grave pour l'ordre public.

---

<sup>76</sup> Anafé, [Persona non grata - Conséquences des politiques sécuritaires et migratoires à la frontière franco-italienne, Rapport d'observations 2017-2018](#), février 2019, p. 86 et s.

<sup>77</sup> Collectif Délinquants Solidaires, [Délit de solidarité : le guide est là !](#), juillet 2019.

<sup>78</sup> TA Nice, 4 mai 2017, n° 1602391.

<sup>79</sup> Les « notes blanches » sont des documents, attribués aux services de renseignement, sans en-tête, ni date, ni référence, ni signature, de façon à protéger le secret des sources. Elles font état de tous les éléments de faits qui « prouvent », selon l'Administration, qu'une personne représente une menace pour la sécurité et l'ordre public.

Le tribunal administratif de Paris a conclu en 2018 à l'absence de menace à l'ordre public, notamment au motif que les faits n'étaient pas établis, ou à tout le moins trop anciens pour être retenus comme une cause de refus d'entrée sur le territoire<sup>80</sup>.

Enfin, en 2019, pour annuler un refus d'entrée pris contre une ressortissante anglaise au port de Douvres par les autorités françaises, le tribunal administratif de Lille a estimé qu'« *il ressort des pièces du dossier, et notamment de la note blanche versée aux débats par le ministre de l'intérieur, que pour refuser l'entrée sur le territoire français de Mme X, les services du ministère de l'intérieur se sont fondés sur la circonstance qu'elle représenterait une menace pour l'ordre public, dans la mesure où elle est membre de la mouvance « no border » et susceptible de se livrer à des actions violentes [fondés sur des faits intervenus en 2010]. Toutefois, Mme X soutient qu'elle n'a commis aucune infraction pénale durant cette manifestation et n'a pas fait l'objet de poursuite. Par ailleurs, la note produite par le ministre, se bornant à mentionner une interpellation de l'intéressée durant une manifestation en Grande-Bretagne, le 26 mars 2011, n'apporte pas de précisions suffisantes sur les faits qu'elle aurait commis durant cet événement et qui seraient de nature à établir l'existence d'une menace pour l'ordre public. En outre, [les faits datés de 2010] sur lesquels repose la décision contestée ne permettent pas, compte tenu de leur nature et de leur ancienneté, d'établir que l'intéressée représenterait une menace réelle, actuelle et suffisamment grave pour l'ordre public de nature à justifier à l'égard d'un ressortissant d'un Etat membre de l'Union européenne un refus d'entrée sur le territoire français* »<sup>81</sup>.

Ces situations ne sont pas isolées et sont révélatrices des dérives de la police et de l'administration en matière de surveillance et de contrôle des activités militantes. A quand une généralisation à l'ensemble de la population européenne ?

---

<sup>80</sup> TA Paris, 25 octobre 2018, n° 1707798/4-1. « [Mésusage des notes blanches et fichage de citoyens européens - Le tribunal administratif de Paris annule le refus d'entrée en France visant un militant solidaire des personnes exilées](#) », Communiqué Anafé – GISTI, 26 novembre 2018.

<sup>81</sup> TA Lille, 19 mars 2019, n° 1704597.